



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,904	01/14/2004	Marc A. Boulanger	RPS920030037US1	3081
45211 7590 06/20/2007 Robert A. Voigt, Jr. WINSTEAD SECHREST & MINICK PC PO BOX 50784 DALLAS, TX 75201			EXAMINER SCHMIDT, KARI L	
			ART UNIT 2139	PAPER NUMBER
			MAIL DATE 06/20/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No. 10/756,904	Applicant(s) BOULANGER ET AL.	
	Examiner Kari L. Schmidt	Art Unit 2139	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 14 January 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>1/14/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by  
Shanklin et al. (US 6,578,147).

#### Claim 1

Shanklin discloses a method for rapid intrusion detection for network communication comprising the steps of:

receiving packets of network data in a network processor coupled to a network fabric (column 3, lines 10-18: "receives and sends data in "packets" which are switched between network segments by router");

forwarding routed network data to the network fabric; and coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data (column 2, lines 59 – column 3, line 3: "each

Art Unit: 2139

sensor is identical to the other sensors and is capable of performing the same intrusion detection processing. The sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a signature that matches on of a collection of known intrusion signature..").

### Claim 2

Shanklin discloses the method of claim 1, further comprising the steps of: storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected (column 6, lines 25-46: "each sensor has a unique IP address" and column 1, lines 50-60: "one known pattern of unauthorized access is associated with "IP spoofing" whereby an intruder sends a message is from a trusted port. To engage in IP spoofing, the intruder must first use a variety of techniques to find a IP address of a trusted port and must then modify the packet headers so that it appears that the packets are coming from that port. This activity result in a signature that can be detected when matched to a previously stored signature of the same activity"); and storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures ("column 4, lines 54-61: "sensor contains a detection engine... the sensor also analyzes each packet's relationship to adjacent and related packets in the data stream and if the analysis indicates misuse the sensor may act autonomously to take action, such as disconnection..").

Art Unit: 2139

Claim 3

Shanklin discloses the method of claim 2, further comprising the steps of:

analyzing the packets of network data for validity thereby generating valid

packets of network data as the selected data (column 6, lines 9-24: "session analyzer

which stores information used to detect signatures from different packets in the same

session... For example, a first sensor might receive a packet indicating a signature that would be comprised of different packets from the same session...");

comparing the selected data to the store N intrusion signatures and generating, at

network data speed, a pattern compare signal and particular ID data when a particular

one of the N intrusion signatures is detected (column 2, lines 59 – column 3, lines 1-3: "

sensors operate in parallel and analyze packets to determine if any packet or series of

packets has a signature that matches one of a collection of known intrusion signatures...

invention provides an easily scalable solution to providing an intrusion detection system

whose ability to perform signature analysis can keep up with high speed networks;

column 7, lines 29-39) ; and

executing the action code corresponding to the particular one of the N intrusion

signatures detected ("column 4, lines 54-61: "sensor contains a detection engine... the

sensor also analyzes each packet's relationship to adjacent and related packets in the

data stream and if the analysis indicates misuse the sensor may act autonomously to

take action, such as disconnection..").

Claim 4

Shanklin discloses the method of claim 3, wherein the PPDE comprises:

an input/output (I/O) interface for coupling data into and out of the PPDE;

M' processing units (PUs), each of the M PUs having compare circuitry for

comparing each of the sequence of input data to pattern data stored in each of the M PUs and generating a compare output, wherein an address pointer selecting the pattern data in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data;

an input bus for coupling the sequence of input data to each of the M PUs in parallel;

an output bus coupled to the I/O interface for sending output data to the I/O interface;

control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M processing units; and

ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, wherein the match ID and

match data corresponding to the match ID are saved in a temporary register as the

output data (Figure 4 and column 7, lines 1-27: "a switch having internal intrusion

detection sensors.. packets are forwarded by switch based on destination address and

the operation of switch is such that its control unit ensures that only packets having a

certain address are output from the port...").

Art Unit: 2139

Claim 5

Shanklin discloses the method of claim 3, wherein the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data ( Figure 4, column 4, lines 54-61: "sensor contains a detection engine, which examines each packet incoming to the sensor including its header and payload. The sensor also analyzes each packet's relationship to adjacent and related packets in the data stream..." column 4, lines 54-61: "sensor contains a detection engine... the sensor also analyzes each packet's relationship to adjacent and related packets in the data stream and if the analysis indicates misuse the sensor may act autonomously to take action, such as disconnection..").

Claims 6-20

The system and method claims are one of the same therefore rejected for the same reason as the method claims above.

**Conclusion**

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Milliken (US 2003/0115485 A1) teaches hash-based systems and methods for detecting, preventing and tracing network worms and viruses.

Buer et al. (US 2004/0143734 A1) teaches data path security processing.

Buer et al. (US 2004/0139313 A1) teaches tagging mechanism for data path security processing.

Stephenson (US 2005/0076236 A1) teaches method and system for responding to network intrusion.

Oh et al. (US 2005/0125551 A1) teaches high-speed pattern storing and matching method.

Lingafelt et al. (US 2004/0199790 A1) teaches use of a programmable network processor to observe a flow of packets.

Ye et al. (US 6, 907, 436 B2) teaches method for classifying data using clustering and classification algorithm supervised.

Kreibich, Christian. Honey-Creating Intrusion Detection Signatures Using Honeypots. 2003 Oct. 31. <http://www.sigcomm.org/HotNets-II/papers/honeycomb.pdf>.

Sommer, Robin. Enhancing Byte-Level Network Intrusion Detection Signatures with Context. 2003 Aug 18. <http://www.icir.org/vern/papers/sig-ccs03.pdf>.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

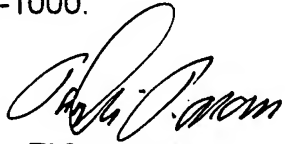
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

  
TAGHI ARANI  
PRIMARY EXAMINER  
3/25/04